MICROTECH

Relatório Técnico de Ajustes, Segurança e Conformidade

Ambiente FÁCIL - Análise Técnica e Pentest

Padrão de referência: ISO/IEC 27001, boas práticas de segurança da informação e aderência LGPD

Finalidade do documento
Este relatório é destinado à equipe técnica e aos responsáveis pela sustentação do ambiente. O objetivo é detalhar os ajustes recomendados, os pontos de atenção identificados, os riscos técnicos e os controles sugeridos para evolução da segurança, disponibilidade, rastreabilidade e governança do ambiente FÁCIL.

Campo	Descrição
Cliente	FÁCIL
Preparado por	Microtech
Tipo de documento	Relatório técnico - não executivo
Escopo aprovado	Análise técnica da infraestrutura + execução de Pentest
Versão	1.0

Sumário

1. Escopo técnico aprovado

O cliente aprovou duas frentes de trabalho complementares: a realização de uma análise técnica da infraestrutura e a execução de um Pentest. Este relatório consolida os ajustes técnicos recomendados a partir dessas duas frentes, com foco operacional, segurança da informação, continuidade, rastreabilidade e conformidade.

Frente aprovada	Descrição técnica	Resultado esperado
Análise técnica da infraestrutura	Mapeamento geral do ambiente, incluindo firewall local, firewall cloud, servidores, VPN, TSplus/RDP, links, sistemas críticos, serviços publicados, cloud e evidências operacionais.	Identificar problemas, riscos operacionais, dependências, gargalos, falhas de configuração e oportunidades de melhoria técnica.
Pentest	Avaliação de segurança focada na superfície exposta, IPs públicos, serviços publicados, FreePBX, portas, NATs, componentes desatualizados e vetores de exploração.	Identificar vulnerabilidades técnicas, severidade, priorização de correções e necessidade de validação após remediação.

Observação técnica
Este documento não substitui políticas formais de segurança, plano de continuidade, inventário oficial de ativos ou processo de gestão de mudanças. Ele deve ser usado como base para criação de plano técnico de correção, revisão mensal e evidências de melhoria contínua.

2. Metodologia e referências de controle

A abordagem utilizada neste relatório considera boas práticas de segurança da informação, gestão de riscos, governança de TI e proteção de dados. A ISO/IEC 27001 é utilizada como referência de controles e estrutura de gestão, sem caracterizar certificação formal do ambiente.

- Levantamento técnico e análise das evidências apresentadas durante o diagnóstico.
- Separação dos pontos em problemas operacionais identificados e vulnerabilidades de segurança identificadas no Pentest.
- Priorização por impacto, criticidade, exposição, recorrência e relação com continuidade operacional.
- Recomendação de controles técnicos e administrativos alinhados a boas práticas de segurança.
- Indicação de evidências esperadas para acompanhamento, auditoria interna e evolução contínua.

Referência	Aplicação prática no relatório
ISO/IEC 27001	Gestão de riscos, controles, responsabilidade, continuidade, monitoramento, controle de acesso, gestão de vulnerabilidades e evidências.
ISO/IEC 27002	Boas práticas de implementação de controles técnicos e administrativos.
LGPD	Proteção de dados pessoais, segurança, prevenção, responsabilização e prestação de contas.
Boas práticas de operação	Monitoramento, patch management, inventário, hardening, gestão de mudanças e análise de incidentes.

3. Diagnóstico técnico consolidado

O ambiente FÁCIL possui infraestrutura operacional e recursos técnicos presentes, porém apresenta necessidade de amadurecimento na gestão contínua de riscos, revisão recorrente de exposição externa, monitoramento ativo, atualização

de componentes e governança técnica. Os problemas identificados não devem ser tratados como eventos isolados; eles precisam ser incorporados a um ciclo mensal de avaliação, correção, documentação e validação.

- A infraestrutura foi mapeada de forma geral, incluindo firewall, cloud, VPN, TSplus/RDP, servidores, sistemas críticos, publicações e serviços expostos.
- Foram identificados problemas operacionais relacionados a acesso remoto, consumo de recursos, dependência de camadas em home office e impacto em telefonia/Discador/CRM Gestão.
- O Pentest apontou vulnerabilidades de alta, média e baixa severidade, com destaque para FreePBX exposto, sistema operacional em fim de vida e necessidade de revisão de patches.
- Há necessidade de padronizar automação de patches, com periodicidade, responsáveis, janela de manutenção, critérios de rollback e evidência de execução.
- É recomendado implantar ou evoluir monitoramento em tempo real, com triggers para sistemas críticos e dashboards executivos/técnicos.

4. Classificação técnica do ambiente

Item	Classificação técnica	Justificativa
Maturidade geral	Média	A infraestrutura sustenta a operação, porém requer evolução em governança, segurança preventiva, monitoramento e gestão contínua de risco.
Risco geral	Médio com pontos de alta criticidade	Existem vulnerabilidades e fragilidades pontuais com potencial de impacto relevante, principalmente em serviços expostos e acesso remoto.
Prioridade de ação	Alta	As correções devem ser priorizadas por risco, iniciando por FreePBX, sistema operacional sem suporte, publicações/NATs e estabilidade do TSplus.
Governança técnica	Em evolução	Necessária criação de rotinas mensais, com comitê de gestão de riscos, acompanhamento de indicadores e formalização de ações.

Interpretação da classificação
A classificação técnica considera o ambiente como operacional e estruturado, porém com riscos acumulados que precisam ser tratados por processo contínuo. A principal evolução recomendada é sair de um modelo reativo para um modelo preventivo, com revisão mensal, dashboards, triggers, evidências e plano de ação por criticidade.

5. Problemas identificados na análise técnica

A análise técnica considerou problemas operacionais identificados e relatados no ambiente, com foco em estabilidade, disponibilidade, experiência do usuário, acesso remoto, consumo de recursos e impacto nos sistemas de negócio.

Problema técnico	Camada afetada	Impacto provável	Tratativa recomendada
Instabilidade em sessões remotas TSplus/RDP	Acesso remoto / Home office	Reconexões, perda de responsividade, falhas perceptíveis em áudio, microfone, USB e aplicações publicadas.	Ajustar políticas de sessão, reduzir redirecionamentos, validar recursos RDP, revisar logs e monitorar sessão por usuário.
Redirecionamento de áudio/USB	TSplus / RDP / VoIP	Áudio instável, falha de microfone,	Avaliar uso de telefonia fora da

sensível em TSplus		impacto em ligações e operação do Discador.	sessão remota, softphone local, WebRTC homologado ou alternativa mais adequada.
Dependência de múltiplas camadas em home office	Internet do usuário / VPN / TSplus / RDP / Aplicação	Dificuldade de isolar causa raiz, pois a falha pode ocorrer em qualquer camada do caminho.	Criar baseline mínimo para home office, validar latência, perda, jitter, banda, VPN e estabilidade local.
Uso elevado de memória no servidor TSplus	Servidor TSplus	Risco de paginação, lentidão e perda de folga operacional conforme aumento de usuários.	Avaliar expansão de memória para 45 GB, monitorar após ajuste e validar redução de paginação.
Picos de CPU e gravação em disco SAS	Servidor TSplus / storage local	Congelamentos momentâneos, aumento de latência e impacto em sessões ativas.	Monitorar processos causadores, fila de disco, paginação, IOPS, latência de disco e horários de pico.
Impacto no CRM Gestão quando Discador falha	CRM Gestão / Discador / Telefonia	Usuários podem perder capacidade de ligação, autenticação de agente, produtividade e fluxo de cobrança.	Separar diagnóstico de CRM, Discador e camada de voz; criar triggers de disponibilidade e procedimento de contingência.
Publicações/NATs a revisar	Firewall local / firewall cloud	Aumento de superfície de ataque e risco de exposição indevida.	Revisar finalidade, origem permitida, destino, porta, responsável, prazo e necessidade de cada regra.
Ausência de processo formal de patches	Servidores e aplicações	Componentes permanecem expostos a falhas conhecidas por mais tempo.	Implantar política de patches com ciclo mensal, janela de manutenção, homologação e evidências.

6. Vulnerabilidades identificadas no Pentest

O Pentest executado identificou vulnerabilidades relacionadas à superfície exposta, serviços publicados e componentes desatualizados. A correção deve seguir priorização por severidade e exposição.

Host/Camada	Vulnerabilidade	Severidade	Correção técnica recomendada
IP Público 186.237.145.229	FreePBX vulnerável a execução remota de comandos	Alta	Atualizar/corrigir FreePBX, restringir origem, validar necessidade de exposição e revisar logs.
IP Público 186.237.145.229	FreePBX com bypass de autenticação administrativa	Alta	Bloquear interface administrativa pública, aplicar patch, revisar credenciais, habilitar MFA quando aplicável.
IP Público 186.237.145.229	FreePBX vulnerável a execução remota de código	Alta	Atualizar aplicação/módulos, restringir portas, revisar módulos e revalidar exposição.
IP Público 186.237.145.229	Sistema operacional CentOS 7 em fim de vida	Alta	Planejar migração para sistema suportado, backup, homologação e substituição controlada.
IP Público 186.237.145.229	Gerenciamento de patches insuficiente em OpenSSH/Apache/MySQL/PHP	Média	Atualizar componentes, validar compatibilidade, aplicar hardening e registrar evidências.
Firewall Local / VPN SSL	Ausência de MFA, geoblock e política adequada de sessão	Média	Implementar MFA, restrição geográfica quando aplicável, limite de sessão e logs de acesso.
Firewall Local / NAT	Publicações externas e origens permitidas a revisar	Média/Baixa	Revisar regras, restringir origem, remover regras sem uso e documentar finalidade.

Firewall Cloud / Serviços	Parâmetros TLS e hardening a revisar	Média	Revisar protocolos, cipher suites, certificados, headers e exposição administrativa.

7. Plano técnico de tratamento por domínio

7.1 Governança de riscos e melhoria contínua

Recomenda-se a criação de um Comitê de Gestão de Crises, Riscos e Melhoria Contínua, com participação técnica e executiva, para tratar riscos, continuidade operacional, indicadores, priorizações e evolução do ambiente.

- Reunião mensal de revisão de riscos, pendências e indicadores críticos.
- Registro de plano de ação com responsável, prazo, prioridade, status e evidência de conclusão.
- Revisão de riscos após mudanças relevantes em firewall, cloud, VPN, TSplus e sistemas críticos.
- Acompanhamento de indicadores: disponibilidade, incidentes, uso de recursos, patches aplicados, vulnerabilidades pendentes e eventos críticos.

7.2 Gestão de patches

- Criar calendário mensal de patches para sistemas operacionais, aplicações, FreePBX, Apache, PHP, MySQL/MariaDB, OpenSSH e componentes de infraestrutura.
- Definir janelas de manutenção, responsáveis, critérios de homologação e rollback.
- Classificar patches por criticidade: crítico, alto, médio e baixo.
- Gerar evidências: data de aplicação, host, versão anterior, versão nova, responsável, validação pós-mudança e incidentes relacionados.
- Priorizar componentes em fim de vida ou sem suporte oficial.

7.3 Firewall local, firewall cloud e NATs

- Inventariar todas as regras de NAT/publicação com origem, destino, porta, serviço, justificativa, responsável e validade.
- Remover regras sem uso ou sem justificativa operacional.
- Restringir origem sempre que possível, evitando exposição para qualquer origem na internet.
- Separar regras críticas de regras temporárias e aplicar revisão mensal.
- Habilitar logging em regras sensíveis, respeitando retenção e privacidade.
- Padronizar nomenclatura de objetos e regras no firewall local e cloud.

7.4 Acesso remoto, VPN e MFA

- Implementar MFA para VPN e priorizar usuários com perfil administrativo ou acesso a sistemas críticos.
- Avaliar bloqueio por geolocalização e restrição por origem quando aplicável.
- Revisar sessões simultâneas, tempo de sessão, lockout e política de senha.
- Avaliar evolução do modelo SSL-VPN para IPsec VPN/ZTNA quando fizer sentido para segurança, rastreabilidade e escalabilidade.

7.5 Servidores cloud e hardening

- Criar baseline mínimo de hardening para Windows e Linux.
- Revisar firewall local dos servidores, serviços habilitados, portas abertas e usuários administrativos.
- Padronizar antivírus/EDR, logs, NTP, backup, inventário e monitoramento.
- Aplicar segregação por função sempre que possível.

8. Monitoramento ativo, triggers e dashboards em tempo real

Recomenda-se evoluir o ambiente para monitoramento ativo com dashboards em tempo real e triggers automatizadas, permitindo atuação preventiva e redução do tempo de identificação de incidentes.

Camada	Trigger recomendada	Severidade sugerida	Ação esperada
Sistemas críticos	Sistema indisponível ou tempo de resposta acima do limite	Alta/Crítica	Notificar equipe, validar serviço, registrar incidente e acionar responsável.
Links e internet	Link indisponível, perda de pacotes ou latência elevada	Alta	Validar operadora, rota, failover e impacto em VPN/TSplus.
VPN	Túnel desconectado, erro recorrente ou aumento de falhas de autenticação	Alta	Validar firewall, autenticação, origem, logs e disponibilidade.
Servidor TSplus	Memória acima de 85%, CPU elevada, fila de disco ou disco com baixa folga	Média/Alta	Analisar processos, sessões, paginação e capacidade.
Disco	Espaço livre menor que 15% ou latência alta	Alta	Liberar espaço, revisar crescimento e planejar expansão.
CRM/Discador	Falha de login de agente, indisponibilidade do discador ou erro de conexão	Alta	Acionar responsável pela aplicação/telefonia, validar VoIP e sessão.
FreePBX	Serviço parado, porta exposta alterada, falha SIP ou consumo anormal	Alta	Validar serviço, logs, firewall e exposição externa.
Patches	Host sem patch crítico aplicado no prazo	Média/Alta	Abrir ação corretiva e registrar exceção formal se necessário.

9. TSplus, RDP, home office, áudio, USB, VoIP e CRM Gestão

O cenário de home office possui múltiplas camadas sensíveis: internet do usuário, Wi-Fi local, computador pessoal/corporativo, VPN, firewall, link da empresa, TSplus/RDP, redirecionamento de dispositivos, áudio, microfone, USB, telefonia/VoIP, Discador e CRM Gestão. Por isso, a falha percebida pelo usuário pode ser consequência de qualquer ponto dessa cadeia.

Ponto técnico crítico
Há indícios de sensibilidade no redirecionamento de áudio, microfone, USB e VoIP dentro da sessão TSplus/RDP. Mesmo quando a VPN permanece conectada, instabilidades rápidas, perda de canais virtuais RDP ou oscilação de internet do usuário podem impactar diretamente áudio, Discador e CRM Gestão.

Item	Risco técnico	Ajuste recomendado	Evidência esperada
Redirecionamento de áudio/microfone	Falhas de áudio e microfone durante atendimento ou uso de Discador.	Reduzir redirecionamentos, testar configuração por grupo e avaliar telefonia local no endpoint.	Logs RdpCoreTS, eventos TSplus, teste controlado com/sem redirecionamento.
USB e dispositivos locais	Instabilidade em canais virtuais e	Desabilitar redirecionamentos não	Comparativo de estabilidade

	aumento de sensibilidade da sessão.	necessários e manter apenas recursos obrigatórios.	antes/depois da alteração.
Internet do usuário	Jitter, perda de pacotes e Wi-Fi doméstico podem causar falhas intermitentes.	Definir requisitos mínimos de home office e checklist de conectividade.	Teste de latência, perda, jitter, velocidade, Wi-Fi/cabeado.
Servidor TSplus	Memória em 90%/97%, risco de paginação e gargalo com mais usuários.	Avaliar aumento para 45 GB e monitorar pós-ajuste.	Gráficos de memória, paginação, CPU, disco e sessões.
Disco SAS	Picos de gravação podem afetar responsividade das sessões.	Monitorar fila de disco, IOPS, latência e processos causadores.	Dashboard com latência de disco, fila e processos por horário.
CRM Gestão / Discador	Quando o Discador falha, há impacto direto na operação de cobrança, produtividade e atendimento.	Separar diagnóstico entre CRM, Discador, VoIP e sessão remota; criar contingência.	Evidência de falha de agente, logs da aplicação, testes de chamada e status do serviço.

Recomenda-se avaliar alternativas para telefonia e Discador, como softphone local no endpoint, WebRTC homologado, telefonia fora da sessão remota ou outro modelo que reduza dependência de áudio e USB redirecionados pelo TSplus. A decisão deve considerar segurança, suporte, aderência operacional e experiência do usuário.

10. Matriz ISO 27001 / LGPD e evidências esperadas

A tabela abaixo relaciona os principais ajustes técnicos com controles de referência de segurança da informação e princípios da LGPD. A relação é orientativa e deve ser adaptada ao Sistema de Gestão de Segurança da Informação da organização.

Domínio	Controle / referência	Relação LGPD	Evidências esperadas
Gestão de riscos	ISO 27001 - avaliação e tratamento de riscos	Responsabilização e prestação de contas	Matriz de riscos, ata do comitê, plano de ação, aceite de risco.
Gestão de patches	Gestão de vulnerabilidades técnicas e mudanças	Segurança e prevenção	Relatório mensal de patches, exceções, evidência de atualização.
Controle de acesso	Identidade, MFA, privilégios e revisão de acessos	Segurança, prevenção, necessidade	Lista de usuários VPN, grupos, MFA habilitado, logs de acesso.
Firewall e NATs	Segurança de redes, segregação e exposição externa	Segurança e prevenção	Inventário de regras, justificativa, origem, destino e revisão mensal.
Monitoramento	Logging, monitoramento e resposta a eventos	Segurança, prevenção, responsabilização	Dashboards, triggers, alertas, histórico de incidentes e ações.
Continuidade	Backup, disponibilidade e resposta a incidentes	Prevenção e segurança	Plano de continuidade, testes de restore, RTO/RPO e simulações.
TSplus/Home office	Segurança no acesso remoto e uso aceitável	Segurança e prevenção	Política de home office, requisitos mínimos, registros de testes.
CRM/Discador	Disponibilidade de sistemas críticos e rastreabilidade	Segurança, qualidade e prevenção	Logs da aplicação, incidentes, plano de contingência e testes.

11. Roadmap técnico 30/60/90 dias

Prazo	Prioridade	Ações técnicas recomendadas
0-30 dias	Alta	Corrigir exposição do FreePBX, planejar migração do CentOS 7, revisar NATs críticos, validar TSplus, aumentar memória para 45 GB se aprovado, criar triggers básicas para sistemas críticos.

0-30 dias	Alta	Criar inventário de publicações, regras de firewall, serviços expostos, responsáveis e justificativas.
31-60 dias	Média/Alta	Implantar política de patches, rotina mensal de revisão, dashboard técnico e alertas automatizados.
31-60 dias	Média/Alta	Avaliar alternativa de telefonia/Discador fora da sessão TSplus ou solução homologada que reduza dependência de redirecionamento.
61-90 dias	Média	Formalizar comitê de gestão de riscos, indicadores executivos, processo de gestão de mudanças e evidências recorrentes.
61-90 dias	Média	Executar revalidação de segurança após correções e registrar mitigação das vulnerabilidades.

12. Critérios de validação e aceite técnico

Para garantir que as ações sejam efetivas, cada correção deve possuir critério de validação objetiva. Abaixo estão os critérios mínimos recomendados.

- Vulnerabilidades altas corrigidas ou formalmente tratadas com plano aprovado e prazo definido.
- CentOS 7 substituído ou com plano formal de migração e mitigação temporária documentada.
- FreePBX atualizado, com exposição reduzida e acesso administrativo protegido.
- Regras de NAT/publicação revisadas, documentadas e com origem restrita quando aplicável.
- Dashboard com triggers ativo para sistemas críticos, links, VPN, TSplus, memória, disco e serviços essenciais.
- Memória do TSplus revisada para 45 GB, caso aprovado, com monitoramento comparativo antes/depois.
- Redirecionamentos TSplus revisados e recursos não necessários desabilitados por política.
- Telefonia/Discador/CRM Gestão com plano de contingência e monitoramento de disponibilidade.
- Política de patches mensal definida e primeira rodada de atualização executada com evidências.
- Comitê de gestão de riscos estabelecido com pauta, responsáveis, indicadores e acompanhamento mensal.

Conclusão técnica
O ambiente FÁCIL deve evoluir para um modelo de operação preventiva, com gestão mensal de riscos, automação de patches, monitoramento em tempo real, triggers para sistemas críticos, revisão de exposição externa e controle técnico das camadas de acesso remoto. A análise técnica e o Pentest devem ser utilizados como base para o plano contínuo de melhoria, correção e conformidade.

13. Evidências técnicas vinculadas aos itens reportados

Esta seção foi consolidada a partir da página de evidências do portal e inclui somente os pontos reportados. As evidências foram agrupadas por domínio técnico para apoiar a execução dos ajustes, validação com fornecedores e acompanhamento interno da equipe de TI.

Critério de uso das evidências
As evidências abaixo não representam, isoladamente, a correção dos problemas. Elas servem como base documental para análise técnica, validação de arquitetura, revisão de políticas, abertura de chamados com fornecedores e confirmação das ações corretivas.

A.1 Evidências de VPN e acesso remoto

Registros relacionados à conectividade do usuário em home office, FortiClient VPN, RemoteApp e comportamento da sessão durante o acesso remoto.

logvpn01 - VPN conectada durante tentativa de acesso remoto

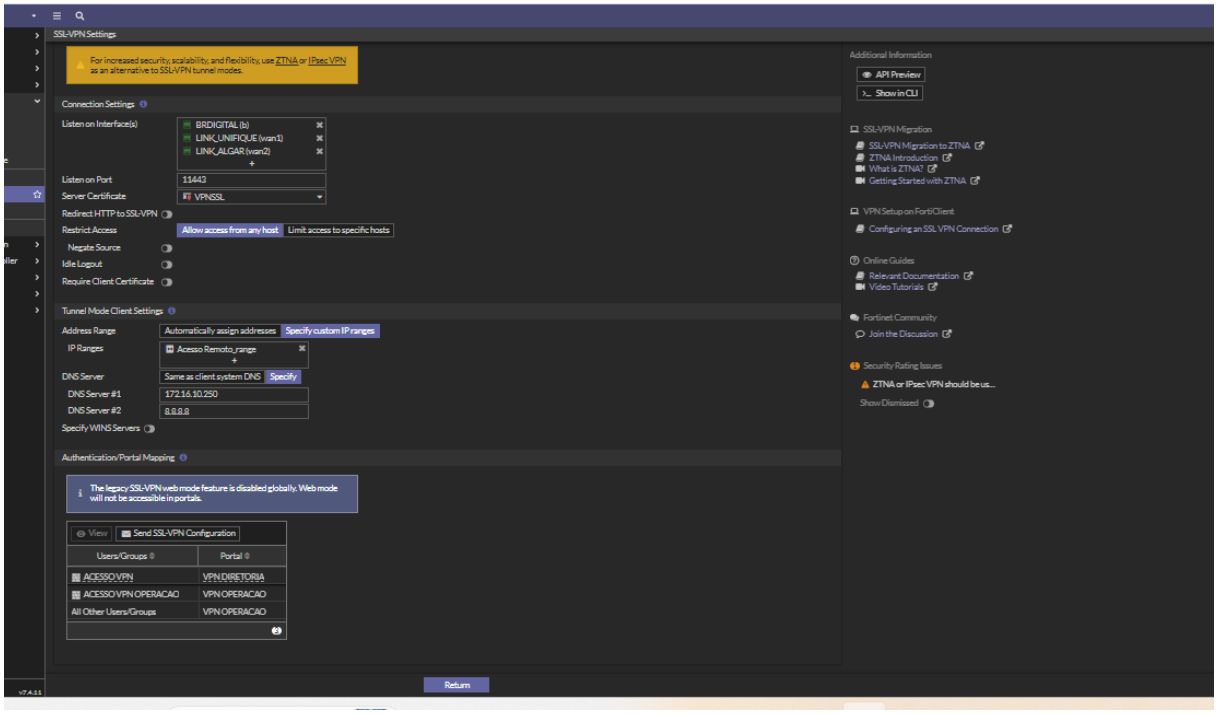
Resumo	Registro visual do FortiClient VPN conectado durante acompanhamento do usuário em home office.
Leitura técnica	A evidência sustenta que havia conexão VPN ativa no momento do registro, enquanto o RemoteApp apresentava tentativa de reconexão.
Risco associado	Instabilidade no TSplus/RemoteApp e dependência da VPN para operação remota.
Tags	VPN, FortiClient, Home office

logvpn02 - Sessão RemoteApp encerrada durante acesso remoto

Resumo	Registro visual de mensagem informando que a sessão de Serviços de Área de Trabalho foi encerrada porque o computador remoto não recebeu nenhuma entrada do usuário.
Leitura técnica	A evidência indica encerramento/desconexão da sessão remota durante o uso do ambiente em home office. O registro reforça o comportamento intermitente percebido pelo usuário, envolvendo a camada de RemoteApp/TSplus, mesmo em cenário de acesso remoto estabelecido.
Risco associado	Instabilidade no TSplus/RemoteApp, encerramento de sessão e impacto na continuidade do trabalho remoto.
Tags	VPN, RemoteApp, Sessão remota, Desconexão

logvpn03 - Configuração de SSL-VPN no FortiGate

Resumo	Registro da configuração de SSL-VPN no FortiGate, contendo interfaces de escuta, porta de acesso, faixa de endereçamento da VPN, DNS e grupos/portais de autenticação.
Leitura técnica	A evidência demonstra que o acesso remoto depende da camada SSL-VPN, com múltiplas interfaces de internet associadas ao serviço. A própria interface do FortiGate também apresenta recomendação para uso de ZTNA ou IPsec VPN como alternativa à SSL-VPN para maior segurança, escalabilidade e flexibilidade.
Risco associado	Dependência do acesso remoto via SSL-VPN, necessidade de avaliação de migração para IPsec/ZTNA e continuidade operacional dos usuários em home office.
Tags	SSL-VPN, FortiGate, Acesso remoto, Recomendação fabricante



Evidência logvpn03: Configuração de SSL-VPN no FortiGate

A.2 Evidências de TSplus, RDP, RemoteApp, áudio, USB e memória

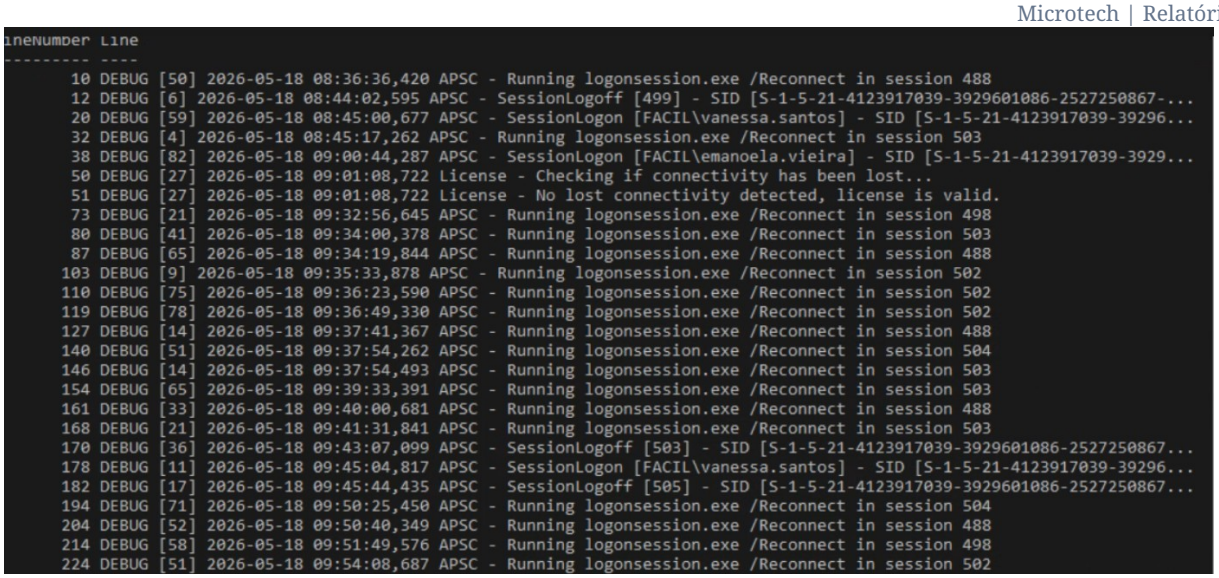
Registros relacionados a reconexão, encerramento de sessão, canais RDP, redirecionamento de áudio/USB, consumo de memória e políticas de sessão.

logts01 - RemoteApp tentando reconectar

Resumo	Evidência visual de usuário com VPN conectada e RemoteApp tentando reconectar ao servidor 172.16.10.241.
Leitura técnica	Indica comportamento de instabilidade na camada TSplus/RemoteApp, mesmo com conectividade VPN ativa.
Risco associado	Instabilidade e reconexão no TSplus para usuários em home office.
Tags	TSplus, RemoteApp, Reconexão

logts02 - Desconexões sucessivas e reconexão posterior de sessão remota

Resumo	Registros de log do TSplus/APSC demonstrando eventos sucessivos de reconexão, logon, logoff e execução do processo logonsession.exe /Reconnect em diferentes sessões.
Leitura técnica	Os eventos analisados demonstram desconexões sucessivas de sessão remota e reconexão posterior. Esse padrão é compatível com perda momentânea de conectividade entre o usuário e o servidor remoto, podendo impactar diretamente recursos sensíveis à sessão, como áudio redirecionado, VoIP, dispositivos USB e estabilidade da aplicação publicada via TSplus.
Risco associado	Instabilidade de sessão remota, reconexões recorrentes, impacto em áudio/USB/VoIP e indisponibilidade parcial para usuários em home office.
Tags	TSplus, Reconnect, SessionLogoff, Sessões instáveis

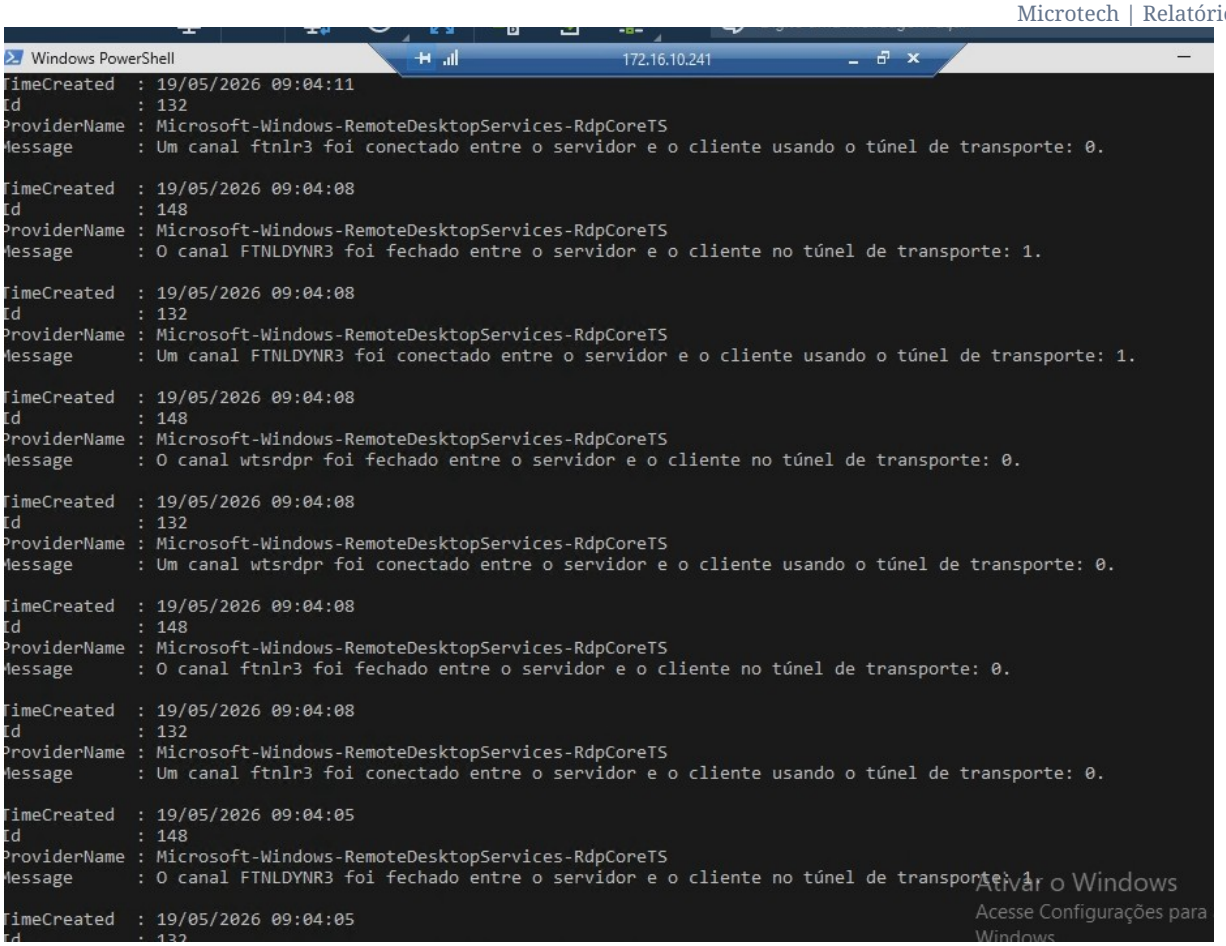


```
LineNumber Line
---------- ----
        10 DEBUG [50] 2026-05-18 08:36:36,420 APSC - Running logonsession.exe /Reconnect in session 488
        12 DEBUG [6] 2026-05-18 08:44:02,595 APSC - SessionLogoff [499] - SID [S-1-5-21-4123917039-3929601086-2527250867-...
        20 DEBUG [59] 2026-05-18 08:45:00,677 APSC - SessionLogon [FACIL\vanessa.santos] - SID [S-1-5-21-4123917039-39296...
        32 DEBUG [4] 2026-05-18 08:45:17,262 APSC - Running logonsession.exe /Reconnect in session 503
        38 DEBUG [82] 2026-05-18 09:00:44,287 APSC - SessionLogon [FACIL\emanoela.vieira] - SID [S-1-5-21-4123917039-3929...
        50 DEBUG [27] 2026-05-18 09:01:08,722 License - Checking if connectivity has been lost...
        51 DEBUG [27] 2026-05-18 09:01:08,722 License - No lost connectivity detected, license is valid.
        73 DEBUG [21] 2026-05-18 09:32:56,645 APSC - Running logonsession.exe /Reconnect in session 498
        80 DEBUG [41] 2026-05-18 09:34:00,378 APSC - Running logonsession.exe /Reconnect in session 503
        87 DEBUG [65] 2026-05-18 09:34:19,844 APSC - Running logonsession.exe /Reconnect in session 488
       103 DEBUG [9] 2026-05-18 09:35:33,878 APSC - Running logonsession.exe /Reconnect in session 502
       110 DEBUG [75] 2026-05-18 09:36:23,590 APSC - Running logonsession.exe /Reconnect in session 502
       119 DEBUG [78] 2026-05-18 09:36:49,330 APSC - Running logonsession.exe /Reconnect in session 502
       127 DEBUG [14] 2026-05-18 09:37:41,367 APSC - Running logonsession.exe /Reconnect in session 488
       140 DEBUG [51] 2026-05-18 09:37:54,262 APSC - Running logonsession.exe /Reconnect in session 504
       146 DEBUG [14] 2026-05-18 09:37:54,493 APSC - Running logonsession.exe /Reconnect in session 503
       154 DEBUG [65] 2026-05-18 09:39:33,391 APSC - Running logonsession.exe /Reconnect in session 503
       161 DEBUG [33] 2026-05-18 09:40:00,681 APSC - Running logonsession.exe /Reconnect in session 488
       168 DEBUG [21] 2026-05-18 09:41:31,841 APSC - Running logonsession.exe /Reconnect in session 503
       170 DEBUG [36] 2026-05-18 09:43:07,099 APSC - SessionLogoff [503] - SID [S-1-5-21-4123917039-3929601086-2527250867...
       178 DEBUG [11] 2026-05-18 09:45:04,817 APSC - SessionLogon [FACIL\vanessa.santos] - SID [S-1-5-21-4123917039-39296...
       182 DEBUG [17] 2026-05-18 09:45:44,435 APSC - SessionLogoff [505] - SID [S-1-5-21-4123917039-3929601086-2527250867...
       194 DEBUG [71] 2026-05-18 09:50:25,450 APSC - Running logonsession.exe /Reconnect in session 504
       204 DEBUG [52] 2026-05-18 09:50:40,349 APSC - Running logonsession.exe /Reconnect in session 488
       214 DEBUG [58] 2026-05-18 09:51:49,576 APSC - Running logonsession.exe /Reconnect in session 498
       224 DEBUG [51] 2026-05-18 09:54:08,687 APSC - Running logonsession.exe /Reconnect in session 502
```

Evidência logts02: Desconexões sucessivas e reconexão posterior de sessão remota

logts03 - Desconexões e reconexões de canais RDP

Resumo	Registros do provedor Microsoft-Windows-RemoteDesktopServices-RdpCoreTS, contendo eventos de abertura e fechamento de canais entre o servidor e o cliente.
Leitura técnica	A evidência apresenta desconexões/reconexões de canais RDP, incluindo fechamento e nova conexão de canais utilizados no túnel de transporte da sessão remota. Esse comportamento é relevante porque canais virtuais do RDP sustentam recursos como áudio, redirecionamento de dispositivos, clipboard, impressoras, drives, câmera e outros componentes da experiência remota.
Risco associado	Instabilidade em canais virtuais do RDP/TSplus, com possível impacto em áudio redirecionado, USB, VoIP, Discador e aplicações publicadas.
Tags	RdpCoreTS, Canais RDP, RemoteApp, Desconexão



Evidência logts03: Desconexões e reconexões de canais RDP

logts04 - Políticas RDP e redirecionamentos habilitados

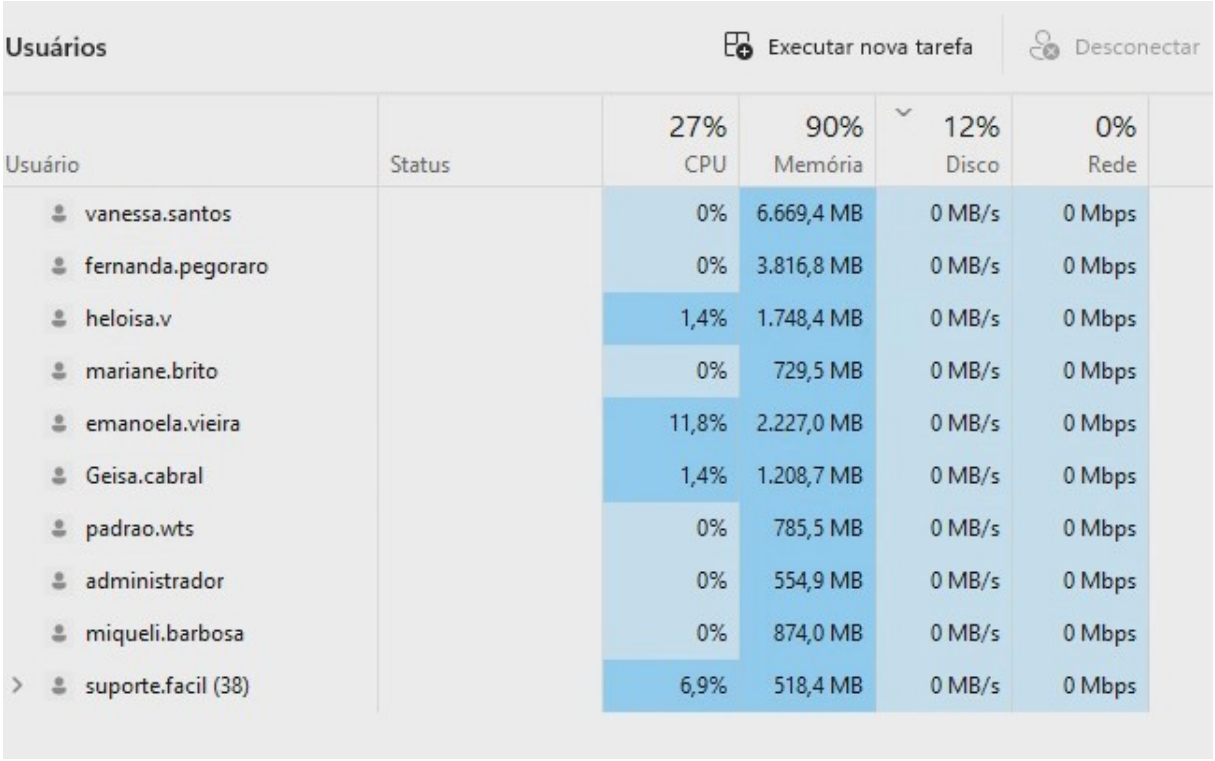
Resumo	Registro de consulta ao caminho de políticas do Terminal Services no Windows, exibindo parâmetros de sessão, tempo de conexão, redirecionamento de áudio, câmera, clipboard, drives, Plug and Play e políticas USB.
Leitura técnica	A configuração analisada não indica limitação de tempo de sessão RDP, pois os valores MaxConnectionTime, MaxDisconnectionTime e MaxIdleTime estão zerados. No entanto, há múltiplos recursos de redirecionamento habilitados, incluindo áudio, câmera, clipboard, drives e Plug and Play, além de políticas específicas de redirecionamento USB. Considerando que os logs do RdpCoreTS registram abertura e fechamento recorrente de canais RDP, o cenário é compatível com instabilidade em canais virtuais do RDP/TSplus, principalmente em usuários home office que utilizam áudio/USB/VoIP dentro da sessão remota.
Risco associado	Alto acoplamento entre sessão remota e recursos redirecionados, podendo gerar instabilidade em áudio, headset, microfone, USB, Discador e VoIP.
Tags	Políticas RDP, Áudio, USB, Redirecionamentos

```
PS C:\Program Files (x86)\TSplus\UserDesktop\files> reg query "HKLM\SOFTWARE\Policies\
 /s

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
    fEnableRemoteFXAdvancedRemoteApp    REG_DWORD    0x0
    fEnableVirtualizedGraphics    REG_DWORD    0x1
    bEnumerateHWBeforeSW    REG_DWORD    0x0
    fEnableWddmDriver    REG_DWORD    0x0
    MaxInstanceCount    REG_DWORD    0xf423f
    AllowSignedFiles    REG_DWORD    0x1
    AllowUnsignedFiles    REG_DWORD    0x1
    fNoRemoteDesktopWallpaper    REG_DWORD    0x0
    fPromptForPassword    REG_DWORD    0x0
    fDisableClip    REG_DWORD    0x0
    fDisableCcm    REG_DWORD    0x0
    fDisableCdm    REG_DWORD    0x0
    fDisableLPT    REG_DWORD    0x0
    fDisablePNPRedir    REG_DWORD    0x0
    VisualExperiencePolicy    REG_DWORD    0x2
    MaxMonitors    REG_DWORD    0x5
    UseUniversalPrinterDriverFirst    REG_DWORD    0x3
    fEnableTimeZoneRedirection    REG_DWORD    0x1
    fAllowUnlistedRemotePrograms    REG_DWORD    0x1
    fTurnOffSingleAppMode    REG_DWORD    0x0
    InitialProgram    REG_SZ
    WorkDirectory    REG_SZ
    MaxDisconnectionTime    REG_DWORD    0x0
    fSingleSessionPerUser    REG_DWORD    0x1
    MaxConnectionTime    REG_DWORD    0x0
    MaxIdleTime    REG_DWORD    0x0
    fDisableAudioCapture    REG_DWORD    0x0
    fDisableCam    REG_DWORD    0x0
    fDisableTerminalServerTooltip    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client
    fEnableUsbBlockDeviceBySetupClass    REG_DWORD    0x1
    fEnableUsbNoAckIsochWriteToDevice    REG_DWORD    0x50
    fEnableUsbSelectDeviceByInterface    REG_DWORD    0x1
```

Evidência logts04: Políticas RDP e redirecionamentos habilitados

logmemoria01 - Servidor TSplus com memória em 90%

Resumo	Registro do Gerenciador de Tarefas demonstrando consumo de memória em aproximadamente 90% no servidor TSplus, com múltiplas sessões de usuários ativas.
Leitura técnica	A evidência demonstra baixa margem operacional de memória no servidor de sessões. Apesar de não indicar falha imediata isoladamente, o consumo elevado pode contribuir para paginação, picos de disco e perda de responsividade em momentos de maior carga. A tela apresenta CPU em aproximadamente 27%, memória em 90%, disco em aproximadamente 12% e múltiplos usuários conectados, com sessões individuais consumindo memória relevante, incluindo usuário com consumo superior a 6 GB.
Risco associado	Alto consumo de memória no servidor TSplus, possível paginação em disco SAS, lentidão intermitente e redução da estabilidade das sessões remotas.
Tags	TSplus, Memória 90%, Sessões RDP, Disco SAS



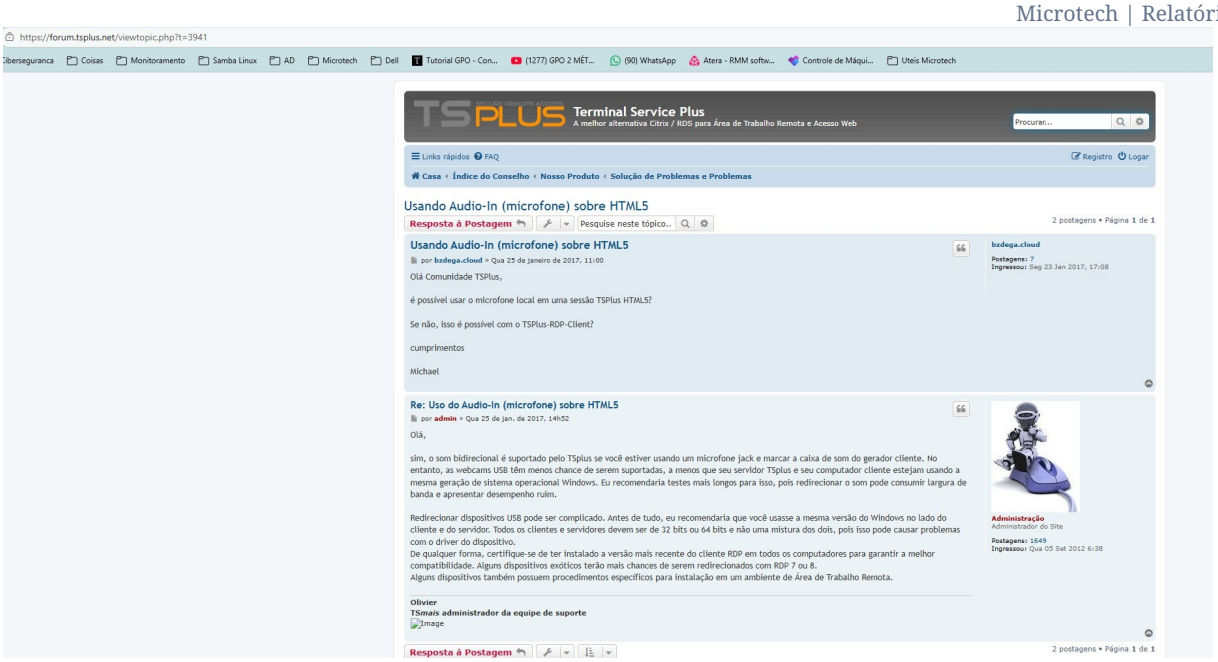
Evidência logmemoria01: Servidor TSplus com memória em 90%

logmemoria02 - Servidor TSplus com pico de memória em 97%

Resumo	Nova evidência do Gerenciador de Tarefas demonstrando aumento do consumo de memória do servidor TSplus, atingindo aproximadamente 97%.
Leitura técnica	A evidência reforça que o servidor está operando com margem operacional extremamente reduzida de memória. Com consumo próximo de 100%, o ambiente pode ficar mais suscetível a paginação em disco, perda de responsividade, lentidão intermitente e impacto nas sessões remotas. Em servidores TSplus/RDP, consumo de memória em 97% é um ponto de atenção relevante, principalmente quando existem múltiplos usuários conectados, aplicações publicadas, redirecionamento de áudio, dispositivos USB, Discador e VoIP dentro da sessão remota.
Risco associado	Servidor TSplus próximo do limite de memória, possível aumento de paginação em disco SAS, lentidão nas sessões, travamentos momentâneos e maior sensibilidade dos canais RDP.
Tags	TSplus, Memória 97%, Sessões RDP, Paginação, Disco SAS

logtsplusaudio01 - Orientação do fórum TSplus sobre áudio/microfone

Resumo	Registro do fórum TSplus abordando o uso de Audio-In/microfone sobre HTML5 e a complexidade do redirecionamento de dispositivos USB em sessões remotas.
Leitura técnica	A evidência reforça que áudio, microfone e dispositivos USB em sessões remotas são pontos sensíveis e podem consumir largura de banda, exigir compatibilidade entre cliente/servidor, versões compatíveis de Windows e testes mais longos para validação.
Risco associado	Telefonia dentro do TSplus, redirecionamento de áudio USB, instabilidade de voz e limitação técnica conhecida da arquitetura.
Tags	TSplus, Áudio, Microfone, Limitação técnica



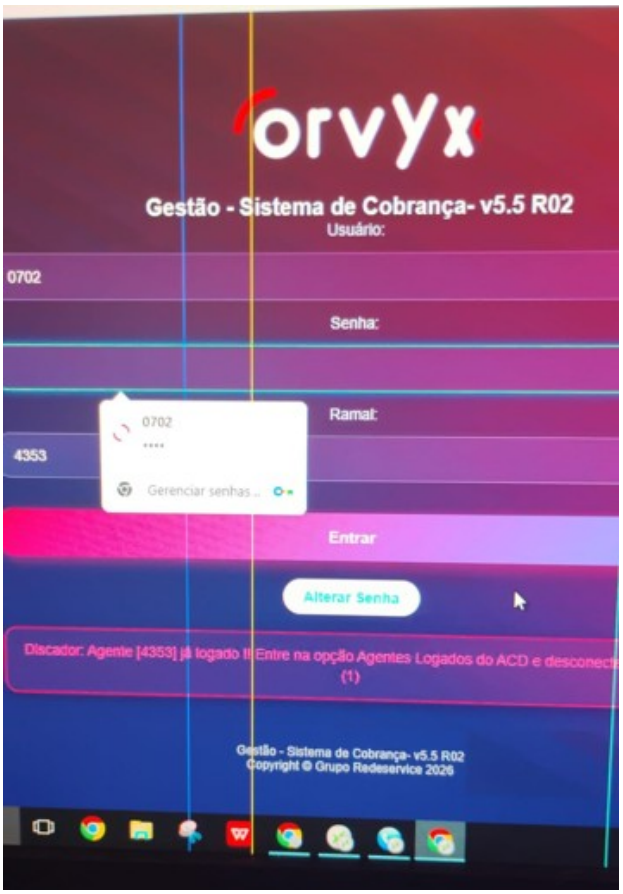
Evidência logtsplusaudio01: Orientação do fórum TSplus sobre áudio/microfone

A.3 Evidências de CRM Gestão e Discador

Registros relacionados ao sistema Orvyx, CRM Gestão, Discador, agentes logados e falhas reportadas durante o uso operacional.

logcrm01 - Discador informa agente já logado

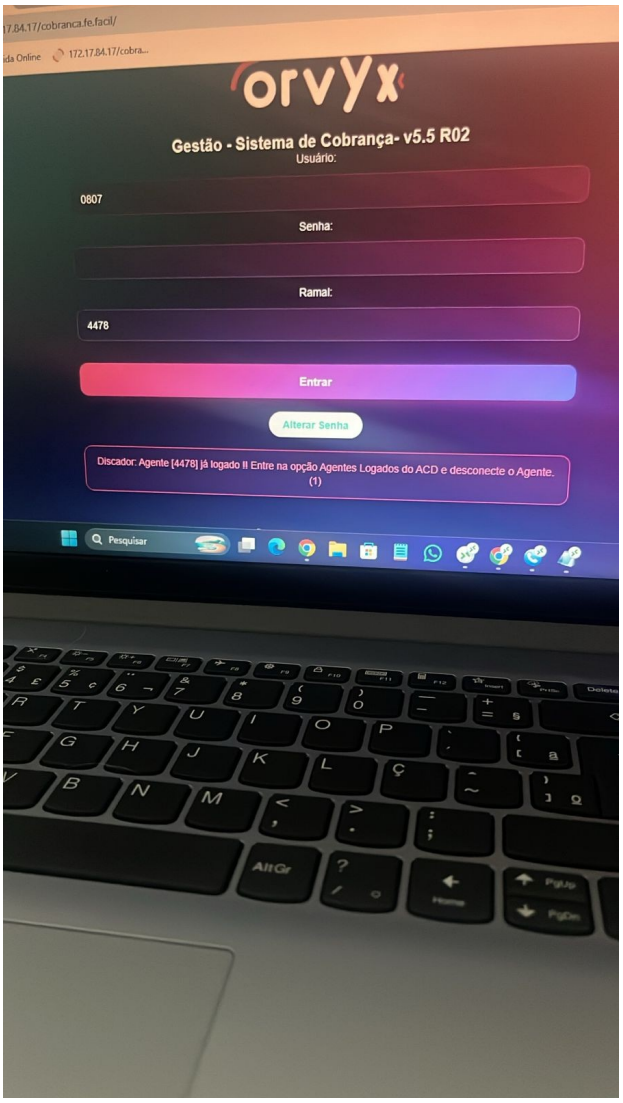
Resumo	Registro do sistema Orvyx / Gestão - Sistema de Cobrança apresentando mensagem de Discador informando que o agente já está logado.
Leitura técnica	A evidência demonstra falha operacional no fluxo de login do Discador, indicando que o sistema reconhece o agente como já conectado e orienta desconexão na opção de agentes logados.
Risco associado	Indisponibilidade parcial do Discador, falha de operação do agente e impacto no uso integrado do CRM Gestão.
Tags	CRM Gestão, Discador, Agente logado, Erro operacional



Evidência logcrm01: Discador informa agente já logado

logcrm02 - Erro recorrente de agente já conectado no Discador

Resumo	Nova evidência do sistema Orvyx / Gestão - Sistema de Cobrança apresentando mensagem de agente já logado, neste caso para outro usuário/ramal.
Leitura técnica	A repetição do comportamento em agentes/ramais diferentes reforça que o problema não parece isolado a um único usuário, podendo estar relacionado ao controle de sessão do Discador, integração com o CRM ou encerramento inadequado de sessões anteriores.
Risco associado	Impacto direto na operação de cobrança, dificuldade de login de agentes e dependência crítica entre CRM Gestão e Discador.
Tags	Discador, Orvyx, Ramal, Agente já logado



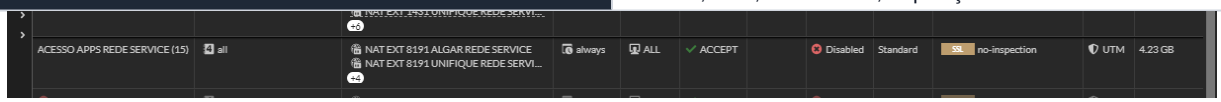
Evidência logcrm02: Erro recorrente de agente já conectado no Discador

A.4 Evidências de firewall e NAT

Registros relacionados ao firewall, NATs, publicações identificadas e exposição de serviços.

logfw01 - NAT / acesso publicado para aplicação RedService

Resumo	Registro do firewall demonstrando regra de acesso para aplicação RedService, com origem ampla e objetos NAT relacionados aos links/operadoras.
Leitura técnica	A evidência indica existência de publicação/acesso externo para serviço relacionado ao ambiente, exigindo atenção quanto à origem permitida, exposição, finalidade da regra e necessidade de revisão periódica.
Risco associado	Exposição de serviço publicado, necessidade de revisão de NATs/regras e controle de origem para acessos externos.
Tags	Firewall, NAT, RedService, Exposição externa



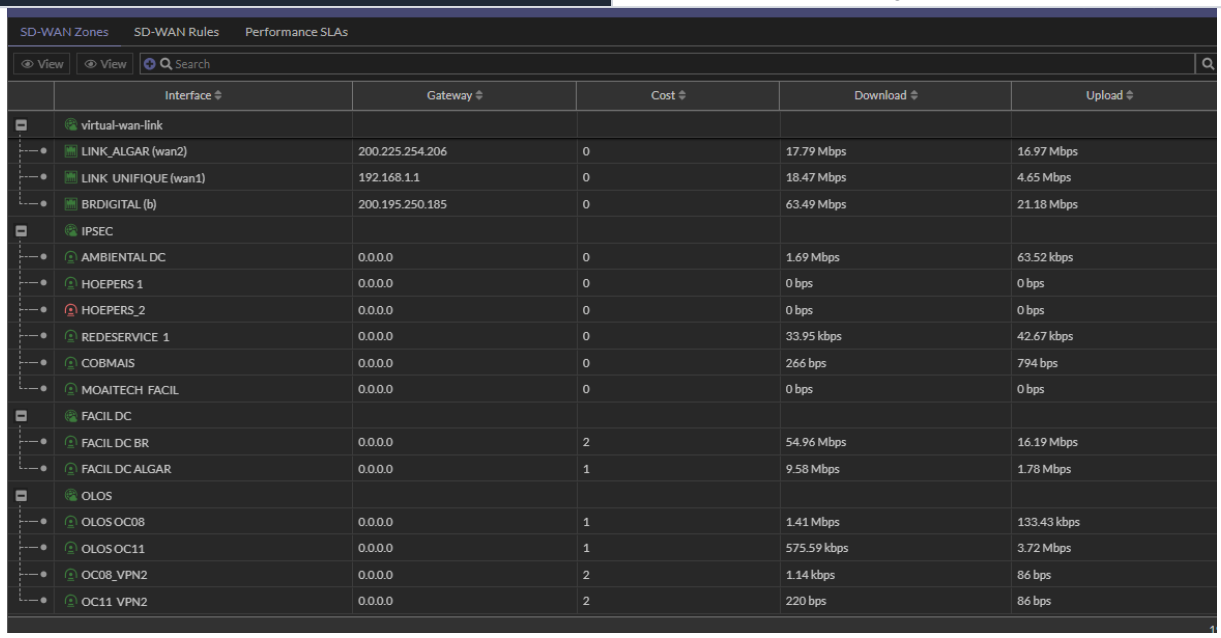
Evidência logfw01: NAT / acesso publicado para aplicação RedService

A.5 Evidências de links, SD-WAN e conectividade

Registros relacionados aos links BrDigital, Unifique, Algar, SD-WAN e testes de comunicação a partir do firewall.

logsdwan01 - SD-WAN com múltiplos links e túneis

Resumo	Registro da tela de SD-WAN do FortiGate demonstrando os links de internet locais e interfaces/túneis associados.
Leitura técnica	A evidência confirma a existência de estrutura com múltiplos links, SD-WAN e tráfego passando por interfaces distintas. No momento analisado, foram observados links ativos com tráfego e túneis VPN associados ao ambiente.
Risco associado	Dependência de conectividade, balanceamento/failover e comunicação entre ambiente local, cloud e usuários remotos.
Tags	SD-WAN, Links, VPN, Tráfego



SD-WAN Zones | SD-WAN Rules | Performance SLAs

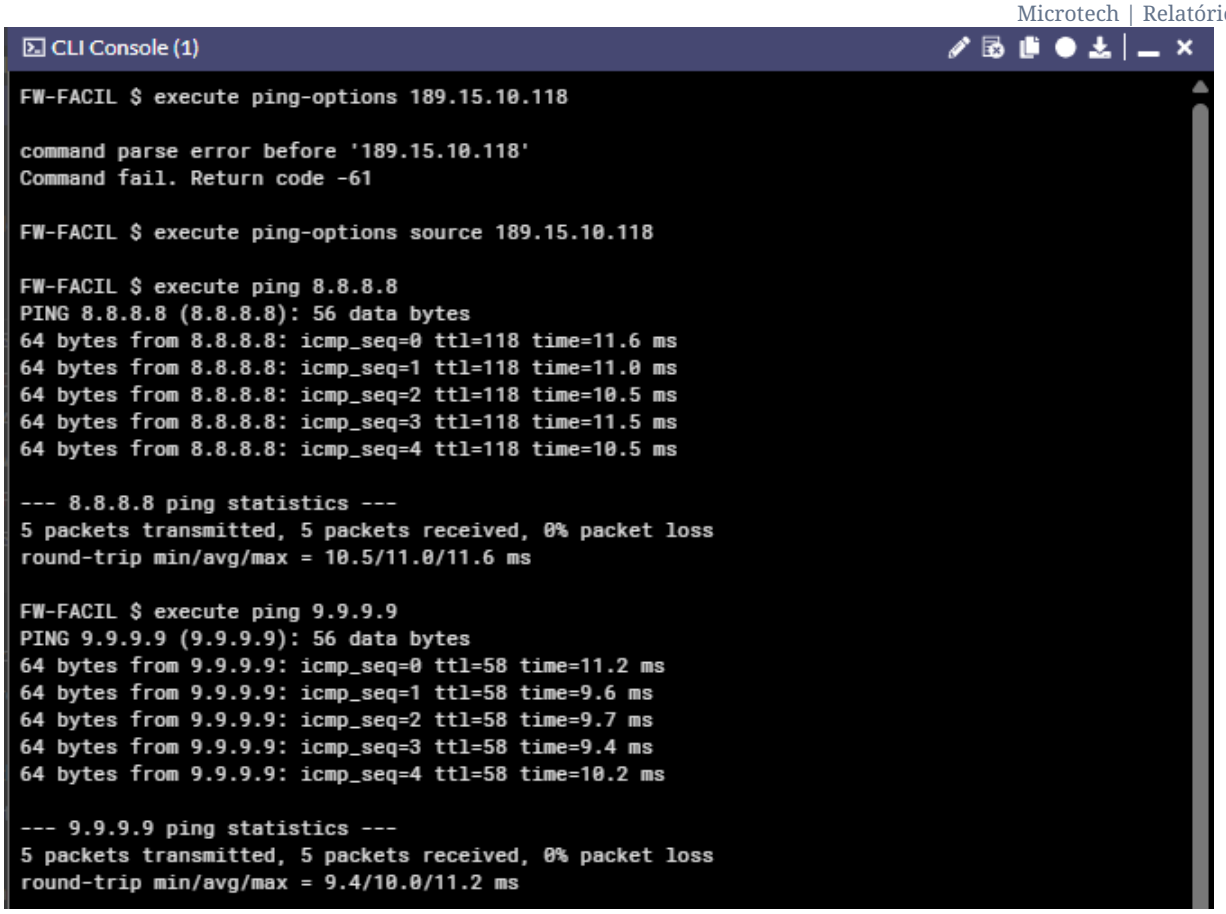
View | View | Search

Interface	Gateway	Cost	Download	Upload
virtual-wan-link				
LINK_ALGAR (wan2)	200.225.254.206	0	17.79 Mbps	16.97 Mbps
LINK UNIFIQUE (wan1)	192.168.1.1	0	18.47 Mbps	4.65 Mbps
BRDIGITAL (b)	200.195.250.185	0	63.49 Mbps	21.18 Mbps
IPSEC				
AMBIENTAL DC	0.0.0.0	0	1.69 Mbps	63.52 kbps
HOEPERS 1	0.0.0.0	0	0 bps	0 bps
HOEPERS_2	0.0.0.0	0	0 bps	0 bps
REDESERVICE 1	0.0.0.0	0	33.95 kbps	42.67 kbps
COBMAIS	0.0.0.0	0	266 bps	794 bps
MOAITECH FACIL	0.0.0.0	0	0 bps	0 bps
FACIL DC				
FACIL DC BR	0.0.0.0	2	54.96 Mbps	16.19 Mbps
FACIL DC ALGAR	0.0.0.0	1	9.58 Mbps	1.78 Mbps
OLOS				
OLOS OC08	0.0.0.0	1	1.41 Mbps	133.43 kbps
OLOS OC11	0.0.0.0	1	575.59 kbps	3.72 Mbps
OC08_VPN2	0.0.0.0	2	1.14 kbps	86 bps
OC11 VPN2	0.0.0.0	2	220 bps	86 bps

Evidência logsdwan01: SD-WAN com múltiplos links e túneis

loglinkalgar - Testes de conectividade pelo link Algar

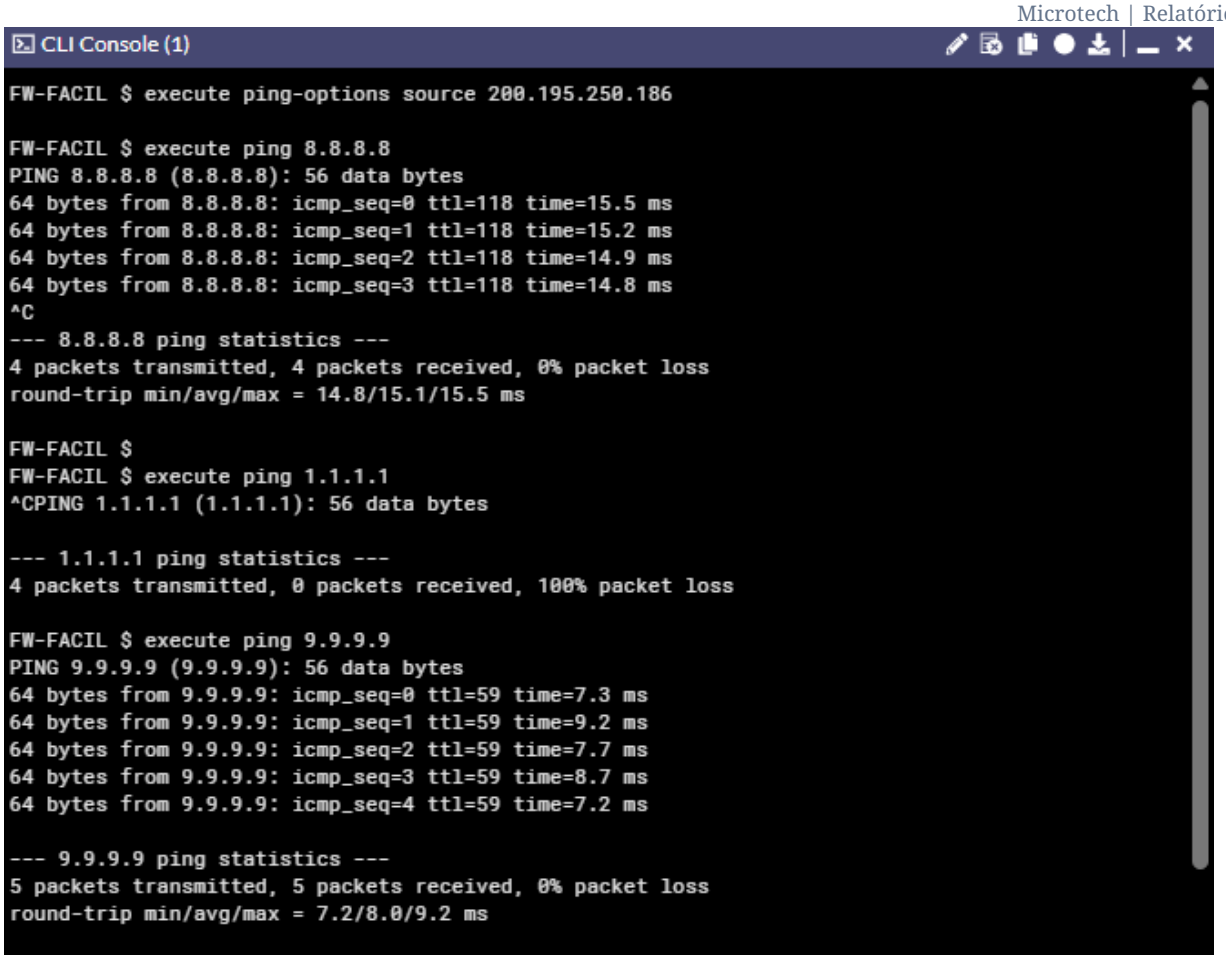
Resumo	Registro de testes ICMP executados a partir do firewall utilizando origem associada ao link Algar.
Leitura técnica	Os testes para destinos como 8.8.8.8 e 9.9.9.9 apresentaram respostas com 0% de perda, indicando conectividade funcional no momento do teste. A tentativa de configuração inicial apresentou erro de sintaxe, mas após ajuste da origem os testes foram executados corretamente.
Risco associado	Validação de conectividade do link, estabilidade de acesso externo e suporte ao SD-WAN.
Tags	Algar, Ping, 0% perda, Conectividade



Evidência loglinkalgar: Testes de conectividade pelo link Algar

loglinkbrdigital - Testes de conectividade pelo link BrDigital

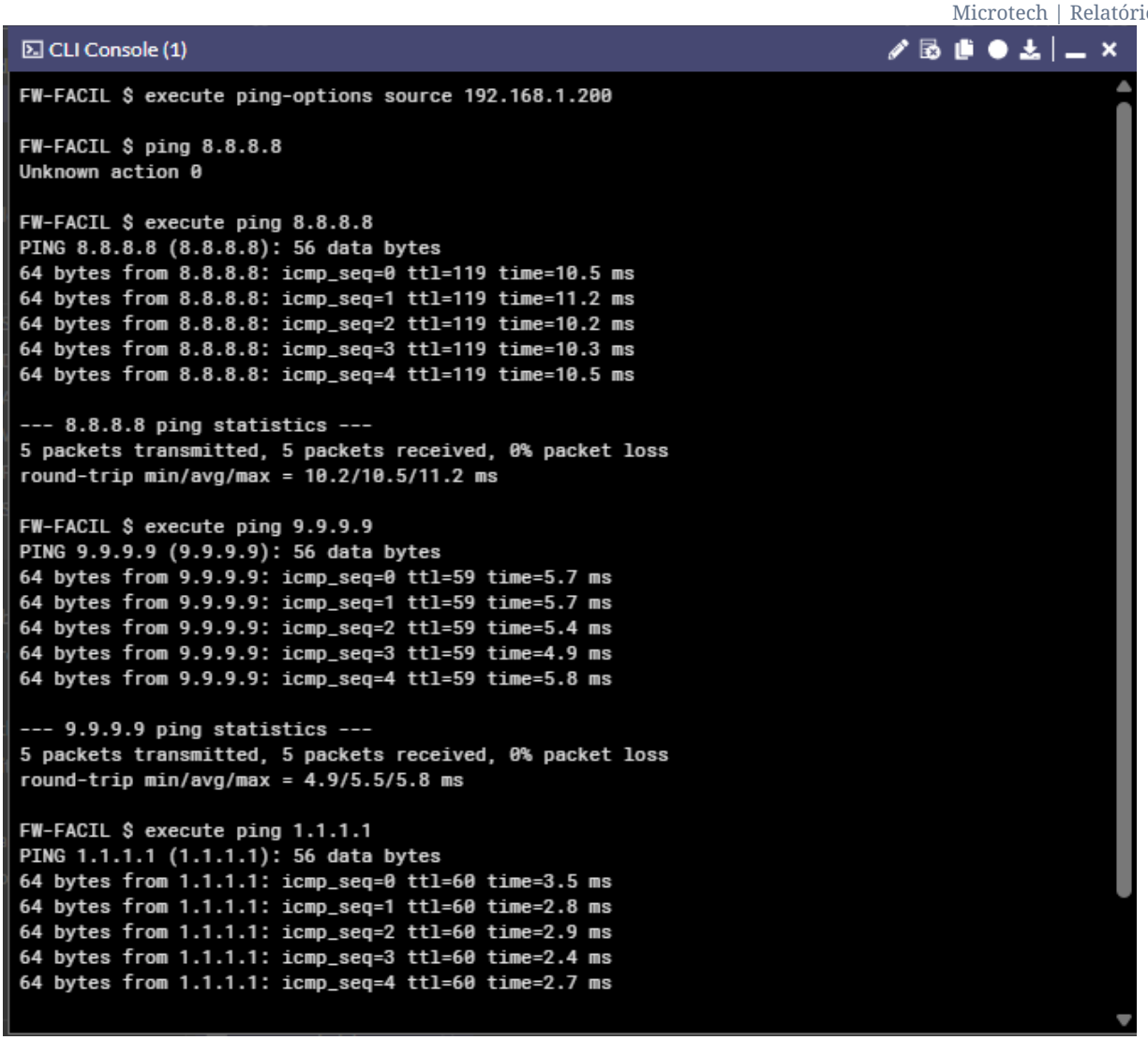
Resumo	Registro de testes ICMP executados a partir do firewall utilizando origem associada ao link BrDigital.
Leitura técnica	Os testes para 8.8.8.8 e 9.9.9.9 apresentaram resposta com 0% de perda. O destino 1.1.1.1 apresentou 100% de perda no momento do teste, podendo representar bloqueio, comportamento específico do destino, rota ou filtro, não necessariamente indisponibilidade geral do link.
Risco associado	Necessidade de avaliar destinos de teste múltiplos e validar conectividade por link sem depender de apenas um endereço externo.
Tags	BrDigital, Ping, 0% perda parcial, 1.1.1.1 sem resposta



Evidência loglinkbrdigital: Testes de conectividade pelo link BrDigital

loglinkunifique - Testes de conectividade pelo link Unifique

Resumo	Registro de testes ICMP executados a partir do firewall utilizando origem associada ao link Unifique.
Leitura técnica	Os testes para 8.8.8.8, 9.9.9.9 e 1.1.1.1 apresentaram respostas com 0% de perda, indicando boa conectividade no momento da validação.
Risco associado	Validação de conectividade do link, operação do SD-WAN e disponibilidade dos acessos externos.
Tags	Unifique, Ping, 0% perda, Conectividade



Evidência loglinkunifique: Testes de conectividade pelo link Unifique

A.6 Evidências de Armazém Cloud, storage e capacidade

Registros relacionados ao ambiente cloud, consumo de disco, file server, capacidade dos servidores e necessidade de relatório complementar.

logdiscofileserver - File server com disco próximo do limite

Resumo	Registro do volume FÁCIL (R:) com aproximadamente 32,5 GB livres de 599 GB, indicando uso elevado de armazenamento.
Leitura técnica	Embora o disco próximo do limite não tenha sido identificado como causa direta da lentidão reportada no TSplus, trata-se de um ponto de atenção preventiva. Ambientes com pouco espaço livre podem apresentar problemas em gravação de arquivos, logs, atualizações, rotinas de backup, performance de aplicações e crescimento operacional.
Risco associado	Capacidade de armazenamento, continuidade operacional do file server e necessidade de acompanhamento preventivo junto ao ambiente cloud/local correspondente.
Tags	Disco, File Server, Capacidade, Atenção preventiva

Evidência logdiscofileserver: File server com disco próximo do limite

logcloud01 - Servidores com disco próximo do limite

Resumo	Registro de servidores com consumo de disco próximo do limite no ambiente hospedado.
Leitura técnica	Embora não tenha sido identificado como causa direta do problema reportado, o ponto deve ser registrado como atenção preventiva.
Risco associado	Dependência da Armazém Cloud, capacidade de disco e continuidade operacional.
Tags	Armazém Cloud, Disco, Capacidade

logcloud02 - Relatório complementar do provedor cloud

Resumo	Item destinado ao registro do relatório complementar da Armazém Cloud, contendo indicadores de desempenho, banda e disponibilidade.
Leitura técnica	O relatório deve ser comparado com monitoramento interno, caso exista, para validar comportamento do ambiente em janela mínima de 7 dias.
Risco associado	Desempenho do ambiente cloud, consumo de banda, disco, IOPS e disponibilidade.
Tags	Cloud, Relatório, Banda

14. Conclusão técnica complementar

Com base nas evidências reportadas, os pontos de maior atenção permanecem concentrados em acesso remoto, TSplus/RDP, redirecionamento de áudio/USB, memória do servidor de sessões, Discador/CRM Gestão, revisão de NATs/publicações, conectividade dos links/SD-WAN e capacidade de armazenamento. O tratamento deve ser conduzido por prioridade, com validação técnica antes e depois de cada ajuste e registro das evidências de aceite.