POLÍTICA DE GESTÃO DE FIREWALL

CREDLEVE

Versão 01 — Minuta para aprovação

Código	PO-04-GF-CL
Data de emissão	31/07/2026
Proprietário	Tecnologia da Informação
Aprovadores	Diretoria / Compliance
Classificação	Uso Interno

1. OBJETIVO

Estabelecer os requisitos técnicos, administrativos e de auditoria para a gestão do firewall corporativo da CREDLEVE, assegurando que alterações de conectividade sejam autorizadas, documentadas, testadas, monitoradas e revisadas, com redução do risco de indisponibilidade, acesso indevido, vazamento de informações e uso inadequado dos recursos de rede.

- Adotar o princípio de menor privilégio e o modelo “negado por padrão, liberado por exceção”.
- Definir responsabilidades para solicitação, análise, aprovação, implementação, validação e revogação de regras.
- Manter trilha de auditoria vinculada ao chamado ou mudança autorizada.
- Assegurar continuidade por meio de redundância de links, cópia de segurança e procedimento de reversão.

2. ABRANGÊNCIA

Esta política aplica-se à sede, filiais, colaboradores, terceiros, prestadores de serviço, equipamentos de rede, servidores, estações, dispositivos conectados, redes sem fio, VPNs e serviços publicados ou consumidos pela CREDLEVE.

3. AMBIENTE DE REFERÊNCIA

A configuração observada na data de elaboração utiliza gateway UniFi UCG Ultra, aplicação UniFi Network 10.5.67, rede interna principal 192.168.1.0/24 e dois provedores de Internet em balanceamento de carga de 50%: Claro NET (WAN1, porta 5) e Vivo (WAN2, porta 4). Os endereços WAN apresentados são privados, indicando a existência de equipamentos dos provedores a montante do gateway.

Componente	Configuração de referência	Diretriz
Gateway	UniFi UCG Ultra	Manter firmware e aplicações em versões estáveis e suportadas.
Rede LAN	192.168.1.0/24	Segmentar servidores, usuários, visitantes, IoT e administração sempre que aplicável.
WAN1	Claro NET — carga 50%	Monitoramento de disponibilidade, latência e perda.
WAN2	Vivo — carga 50%	Monitoramento de disponibilidade, latência e perda.
Roteamento	Duas rotas padrão, métricas equivalentes	Usar balanceamento ou failover conforme criticidade dos sistemas.
NAT	Masquerade para ambas as WANs	Não publicar serviços sem análise, restrição de origem e registro.

4. PRINCÍPIOS E REGRAS GERAIS

1. Todo tráfego não explicitamente permitido deve ser bloqueado.

2. As regras devem utilizar origem, destino, porta e protocolo específicos; “Any/All” somente mediante justificativa e aprovação formal.
3. Regras temporárias devem possuir data de expiração e responsável pela renovação ou remoção.
4. Regras de administração devem ser limitadas à rede de gestão, VPN ou endereços IP confiáveis.
5. Não é permitido expor diretamente interfaces administrativas do firewall, switches, access points ou servidores à Internet.
6. Toda alteração deve possuir plano de teste, plano de reversão e evidência de validação.

5. ARQUITETURA DE ZONAS E MATRIZ DE ACESSO

A matriz abaixo substitui permissões genéricas por acessos mínimos. Novas zonas devem seguir o mesmo princípio.

Origem	Destino	Política padrão	Exceções permitidas
Internal/Usuários	Internet/External	Permitir com inspeção e filtros	Serviços corporativos autorizados; bloqueios por categoria e aplicação.
Internet/External	Internal	Bloquear	Somente sessões de retorno e publicações formalmente autorizadas.
Internal/Usuários	Gateway	Bloquear	DNS, DHCP, NTP e serviços estritamente necessários.
Administração	Gateway/Infraestrutura	Permitir restrito	HTTPS/SSH apenas para administradores autorizados e preferencialmente via VPN.
VPN	Internal	Bloquear por padrão	Liberar somente redes e portas vinculadas ao perfil do usuário.
Visitantes/Hotspot	Internal/Gateway/DMZ	Bloquear	Somente Internet, com isolamento de clientes.
IoT	Internal	Bloquear	Apenas controladores, DNS, NTP e destinos necessários.
DMZ	Internal	Bloquear	Exceções específicas para banco de dados/API, com origem e porta definidas.
Internal	DMZ	Permitir restrito	Somente serviços publicados internamente.

6. CONTROLE DE APLICAÇÕES E CONTEÚDO

A configuração atual contém regras de bloqueio para transferência de arquivos via web e para as aplicações X, Facebook, Netflix, Spotify, TikTok e YouTube. Essas regras deverão ser mantidas ou ajustadas conforme necessidade corporativa, respeitando a ordem de precedência e os grupos de usuários.

Regra sugerida	Ação	Origem	Destino/Aplicação	Observação
CL-BLK-001 Transferência de arquivos web	Bloquear	Rede corporativa	Web File Transfer	Exceção somente por chamado, prazo e usuário/grupo.
CL-BLK-002 Redes sociais	Bloquear	Rede corporativa	Facebook, X e TikTok	Podem existir grupos autorizados para

Regra sugerida	Ação	Origem	Destino/Aplicação	Observação
				Comunicação/Marketing.
CL-BLK-003 Streaming de vídeo	Bloquear	Rede corporativa	Netflix e YouTube	YouTube pode ser liberado por categoria, grupo ou horário.
CL-BLK-004 Streaming de áudio	Bloquear	Rede corporativa	Spotify	Exceções documentadas.
CL-ALLOW-001 Serviços essenciais	Permitir	Rede corporativa	DNS, NTP, atualizações e aplicações de negócio	Deve preceder os bloqueios quando necessário.

7. REDUNDÂNCIA, ROTEAMENTO E NAT

7.1 Links de Internet

- Manter as duas WANs monitoradas por SLA, latência, perda de pacotes e disponibilidade.
- Para sistemas sensíveis a alteração de IP de origem, utilizar roteamento baseado em política para fixação em uma WAN.
- Definir failover automático quando uma WAN estiver indisponível ou acima dos limites de qualidade.

7.2 NAT e publicação de serviços

- Utilizar o formato: IP de origem — IP público/WAN — porta externa — IP interno — porta interna — protocolo.
- Restringir a origem sempre que tecnicamente possível; evitar origem “Any”.
- Preferir VPN, proxy reverso ou serviço de acesso seguro em vez de exposição direta.
- A alteração da porta externa não substitui autenticação forte, atualização, hardening e monitoramento.
- Ativar registro de eventos para regras de publicação críticas.

8. ACESSO ADMINISTRATIVO, SSH E VPN

- A administração da console UniFi deve exigir conta individual, MFA e perfil de privilégio compatível com a função.
- Contas compartilhadas são proibidas, salvo conta de contingência armazenada em cofre e com uso auditado.
- SSH no gateway deve permanecer desabilitado. Quando necessário, deve ser habilitado temporariamente, com senha/chave forte, origem restrita e posterior desativação.
- Acesso remoto deve ocorrer por VPN corporativa, com autenticação individual, revogação imediata no desligamento e revisão periódica dos perfis.
- A VPN não deve conceder acesso irrestrito à rede; regras por usuário ou grupo devem limitar redes, portas e serviços.

9. IDS/IPS, BLOQUEIO GEOGRÁFICO E REGISTROS

- Habilitar IDS/IPS em modo de bloqueio quando a capacidade do equipamento e a validação de desempenho permitirem.
- Manter assinaturas atualizadas e revisar eventos de alta severidade.
- Aplicar bloqueio geográfico de entrada para países sem relação operacional, com exceções formalmente documentadas.
- Registrar eventos de bloqueio, alterações administrativas, VPN, NAT, falhas de link e detecções de segurança.
- Quando houver integração disponível, encaminhar logs para plataforma central de monitoramento/SIEM, com retenção definida pela CREDLEVE.

10. PROCESSO DE SOLICITAÇÃO E ALTERAÇÃO

Toda liberação, bloqueio, NAT, rota, VPN ou alteração de segurança deverá ser solicitada por chamado no GLPI por gestor responsável. O chamado deverá conter, no mínimo:

- Justificativa de negócio e responsável pelo serviço.
- IP/rede de origem e destino.
- Porta(s), protocolo(s) e sentido da comunicação.
- Ambiente e criticidade.
- Prazo de validade da regra, quando temporária.
- Janela de mudança, impacto esperado, teste e reversão.

O técnico responsável analisará o risco e poderá propor solução mais segura. Exceções que contrariem esta política exigem aceite formal do risco pela Diretoria e ciência do Compliance. O nome da regra deverá conter, sempre que possível, o identificador do chamado, o serviço e o responsável.

Etapa	Responsável	Evidência obrigatória
Solicitação	Gestor da área	Chamado completo e justificativa.
Análise técnica e de risco	TI/Segurança	Parecer, escopo mínimo e impacto.
Aprovação	Gestor/TI; Diretoria em exceções	Registro no chamado ou e-mail anexado.
Implementação	Administrador autorizado	Configuração, data, executor e backup prévio.
Teste	TI e solicitante	Resultado técnico e validação funcional.
Encerramento	TI	Evidências, documentação e prazo de revisão.

11. PADRÃO DE NOMENCLATURA E ORDEM DAS REGRAS

As regras devem seguir o padrão: CREDLEVE-[AÇÃO]-[SERVIÇO]-[CHAMADO]-[VALIDADE]. Exemplo: CREDLEVE-ALLOW-ERP-CH12345-20261231.

7. Permissões essenciais e de infraestrutura específicas.
8. Permissões corporativas por aplicação, grupo ou destino.

9. Bloqueios específicos por risco, aplicação ou categoria.
10. Regras temporárias e de exceção, com expiração.
11. Bloqueio final explícito e registro quando aplicável.

12. REVISÃO, CANCELAMENTO E RECERTIFICAÇÃO

- Revisar as regras no máximo a cada seis meses; regras críticas ou temporárias devem ser revisadas com maior frequência.
- Identificar regras sem uso, duplicadas, sobrepostas, excessivamente amplas, sem responsável ou sem chamado associado.
- A regra a cancelar deve ser inicialmente desabilitada, com data, motivo e técnico registrados. Após período de observação, poderá ser removida.
- A revisão deve gerar chamado e relatório com regras incluídas, alteradas, desabilitadas e removidas.

13. BACKUP, CONTINUIDADE E RECUPERAÇÃO

- Manter backup automático semanal da configuração na nuvem UniFi e realizar backup manual antes de mudanças relevantes.
- Testar a restauração periodicamente e sempre após mudança de plataforma ou equipamento.
- Manter inventário de configurações críticas: WANs, VLANs, rotas, VPNs, regras, NAT, administradores e integrações.
- Documentar procedimento de substituição do gateway, contatos dos provedores e configurações necessárias para retomada do serviço.

14. ACORDO DE NÍVEL DE SERVIÇO (SLA)

Serviço	Requisitos mínimos	Baixa	Média	Alta	Setor
Liberação/Bloqueio de acesso	Origem, destino, porta, protocolo e justificativa	4 h	2 h	1 h	TI
Criação/alteração/remoção de NAT	Origem, WAN, porta externa, IP/porta interna e protocolo	4 h	2 h	1 h	TI
Rota ou policy-based routing	Origem, destino, WAN, motivo e impacto	4 h	2 h	1 h	TI
VPN	Usuário/grupo, redes e portas autorizadas, validade	4 h	2 h	1 h	TI
Mudança de configuração	Plano de mudança, teste, reversão e janela	4 h	2 h	1 h	TI

Os tempos acima representam prazo médio para início ou atendimento, contados após o recebimento de todas as informações e aprovações necessárias. Incidentes críticos seguem o processo de resposta a incidentes.

15. RESPONSABILIDADES

Papel	Responsabilidades
Compliance/Segurança	Acompanhar aderência, riscos, auditorias e revisões.
Diretoria	Aprovar a política e aceitar formalmente riscos excepcionais.
Tecnologia da Informação	Administrar o firewall, analisar, implementar, testar, registrar e revisar regras.
Gestores de área	Solicitar, justificar, validar e informar quando o acesso não for mais necessário.
Usuários e terceiros	Utilizar os acessos somente para finalidade autorizada e proteger credenciais.

16. EXCEÇÕES E NÃO CONFORMIDADES

Exceções devem ser temporárias, possuir justificativa, avaliação de risco, controles compensatórios, responsável, prazo de expiração e aprovação formal. Descumprimentos poderão resultar em revogação do acesso, abertura de incidente e aplicação das medidas administrativas cabíveis.

17. REFERÊNCIAS E REGISTROS

- Política de Gestão de Firewall PO-04-GF, versão 08, utilizada como documento de referência.
- Chamados e mudanças registrados no GLPI.
- Planilha ou sistema de Registro de Alterações do Firewall.
- Relatórios semestrais de revisão de regras e evidências de backup/restauração.

18. HISTÓRICO DE REVISÕES

Versão	Data		Revisões	Aprovador	Área
	Emissão	Aprovação			
01	09/02/2026	06/03/2026	Emissão da Política	Marcelo Carmanini	Diretoria