

Troubleshooting

Um ticket foi aberto na empresa esta manhã, o ticket indicava que a maioria dos dispositivos na companhia havia perdido a conexão com a internet, o time N1 tentou aplicar backups da configuração nos ativos e não obteve sucesso, o chamado foi escalado para vocês.

O ticket trás a seguinte informação, os switches não conseguem conectar ao server das cisco para baixar os updates, o SW1 e o SW2 precisam conectar ao site da cisco, é preciso que os switches enviem pings para cisco.com, usando o nome de domínio e o endereço ip.

Como parte do troubleshooting você terá que pegar informação de diferentes fontes, e analisar estas informações para proceder com qualquer plano de resolução, quando a conexão for reestabelecida documente a solução.

Descubra e edite as ACLS para satisfazer os seguintes requerimentos. Todas as ACLs, tem de ser padronizadas com a sequência padrão incrementando o valor de acordo com os requerimentos da empresa, na seguinte ordem.

1. Permitir todos os usuários acessarem apenas o DNS do ISP, outros dns públicos precisam ser bloqueados.
2. Permitir todos usuários acessarem o site da cisco e google apenas em modo seguro, facebook e twitter não são permitidos.
3. Permitir todos os PCs pingarem qualquer dispositivo por qualquer proposito
4. Permitir todos os usuários acesso SSH para recursos externos.
5. Permitir todos os usuários da rede acessarem o gmail, assegure que todos os protocolos tanto de envio quanto de recebimento estejam permitidos.
6. Qualquer outro tráfego precisa ser negado.

Quando estiver testando atenção para que os computadores possam acessar apenas os sites seguros permitidos, mas consigam pingar qualquer destino.

Uma investigação será necessária para permitir que todos os dispositivos possam usar o traceroute, para auxiliar o suporte N1 em suas tarefas. Lembre que a última ACL precisa ser deny any.

Credencias de acesso:

USER: cisco

Password: cisco

Enable: ccna